



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,515	07/06/2001	Michael Freed	NEXSI-01011US0	4141
28863	7590	03/18/2005	EXAMINER	
SHUMAKER & SIEFFERT, P. A. 8425 SEASONS PARKWAY SUITE 105 ST. PAUL, MN 55125			MOORTHY, ARAVIND K	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 03/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	09/900,515	FREED ET AL.
	<b>Examiner</b>	<b>Art Unit</b>
	Aravind K Moorthy	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

1)  Responsive to communication(s) filed on 11 March 2003.

2a)  This action is **FINAL**.                    2b)  This action is non-final.

3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

4)  Claim(s) 1-50 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5)  Claim(s) \_\_\_\_\_ is/are allowed.  
6)  Claim(s) 1-50 is/are rejected.  
7)  Claim(s) \_\_\_\_\_ is/are objected to.  
8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

9)  The specification is objected to by the Examiner.

10)  The drawing(s) filed on 06 July 2001 is/are: a)  accepted or b)  objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All    b)  Some \* c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)  Notice of References Cited (PTO-892)  
2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3)  Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.  
5)  Notice of Informal Patent Application (PTO-152)  
6)  Other: \_\_\_\_\_.  
\_\_\_\_\_

### **DETAILED ACTION**

1. This is response to the communication on 11 March 2003.
2. Claims 1-50 are pending in the application.
3. Claims 1-50 have been rejected.

#### *Specification*

4. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract exceeds the 150-word limit.

#### *Claim Objections*

5. Claims 23 and 41 are objected to because of the following informalities: dependency. A claim cannot depend upon itself. For the sake of examining, the examiner assumes that claim 23 depends upon claim 20 and that claim 41 depends upon claim 33. Appropriate correction is required.

#### *Claim Rejections - 35 USC § 112*

6. Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: step (g) has been omitted from method. For the sake of examining, the examiner assumes that claim 21 begins with step (g) instead of step (h).

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

**7. Claims 1-8, 11 and 45-47 are rejected under 35 U.S.C. 102(e) as being anticipated by Jardin U.S. Patent No. 6,681,327 B1.**

As to claim 1, Jardin discloses a method for secure communications between a client and a server, comprising:

- (a) managing a communications negotiation between the client and the server [column 4, lines 34-47];
- (b) receiving encrypted data packets from the client [column 5, lines 16-30];
- (c) decrypting each encrypted packet data [column 5, lines 16-30];

- (d) forwarding unencrypted data packets to the server [column 5 line 31 to column 6 line 3];
- (e) receiving data packets from the server [column 5 line 31 to column 6 line 3];
- (f) encrypting the data packets from the server [column 5 line 31 to column 6 line 3]; and
- (g) forwarding encrypted data packets to the client [column 5 line 31 to column 6 line 3].

As to claim 2, The method of claim 1 wherein the step of managing comprises:

receiving TCP session negotiation data from the client and modifying the negotiation data prior to forwarding the data to the client [column 4, lines 35-47].

As to claim 3, Jardin discloses modifying a SYN request from the client to the server to alter the packet transmission parameters [column 4, lines 35-47].

As to claim 4, Jardin discloses that the step of modifying includes modifying at least a maximum segment size value of the data packet [column 6 line 58 to column 7 line 5].

As to claim 5, Jardin discloses that the method further includes the steps of negotiating an SSL session with the client [column 6, lines 38-57].

As to claim 6, Jardin discloses that the steps (c) and (f) comprise decrypting SSL encrypted packet data, and encrypting a data packet with SSL [column 6 line 58 to column 7 line 5].

As to claim 7, Jardin discloses the step of managing comprises receiving communication negotiation data directed to the server from the client and responding to the negotiation in place of the server [column 6, lines 4-57].

As to claim 8, Jardin discloses prior to the step (d), of negotiating a separate TCP session with the server [column 4, lines 24-33].

As to claim 11, Jardin discloses prior to the step of receiving encrypted data, of negotiating an encrypted data communications session between an intermediary device and the client [column 4, lines 34-47].

As to claim 45, Jardin discloses an secure sockets layer processing acceleration device, comprising:

a client communication engine establishing a secure communications session with a client device via an open network [column 4, lines 34-47];

a server communication engine establishing an open communications session with a server via a secure network [column 4, lines 34-47]; and

an encryption and decryption engine operable on encrypted data packets received via the open communications session and on clear data received via the open communications session [column 5, lines 16-30].

As to claim 46, Jardin discloses that the client communication engine forwards modified communication session data to at least one server [column 6 line 58 to column 7 line 5].

As to claim 47, Jardin discloses that the client communication engine acts as a proxy for one or more servers in communication with the SSL acceleration device [column 3, lines 46-60].

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**8. Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 as applied to claim 1 above, and further in view of Cohen et al U.S. Patent No. 6,389,462 B1.**

As to claim 9, Jardin does not teach that the step of managing comprises receiving communication negotiation data destined for an intermediary device, altering a destination and source IP addresses of the data, and forwarding the data to the server.

Cohen et al teaches a proxy server that alters a destination and source IP addresses of the data, and forwards the data to the server [column 9 line 19 to column 10 line 31].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin so that there would have been a proxy server that would have altered a destination and source IP addresses of the data and then forwarded the data to the server.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin by the teaching of Cohen et al, as described above, because address translation by a proxy server reduces latency and minimizes traffic onto and off of the network [column 1, lines 44-58].

As to claim 10, Jardin does not teach that the step of receiving communication data comprises the receiving an ACK packet from the server destined for the intermediary device, altering the packet's destination and source IP addresses, and forwarding the packet to the client.

Cohen et al teaches receiving an ACK packet from the server destined for a proxy server, altering the packet's destination and source IP addresses, and forwarding the packet to the client.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin so that the proxy would have received an ACK packet from the server. The proxy server would have altered the packet's destination and source IP addresses, and forwarded the packet to the client.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin by the teaching of Cohen et al, as described above, because address translation by a proxy server reduces latency and minimizes traffic onto and off of the network [column 1, lines 44-58].

**9. Claims 12, 14 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 as applied to claims 1 and 45 above, and further in view of Fujiyama et al U.S. Patent No. 6,052,728.**

As to claims 12 and 48, Jardin does not teach that the step of managing comprises maintaining a database of entries on each session of data packets communicated between the client and the server.

Fujiyama et al teaches maintaining a log of entries on each session of data packets communicated between the client and the server [column 14, lines 9-23].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin so that there would have been a relay computer that would have maintained a log of entries in each session of data packets communicated between the client and the server.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin by the teaching of Fujiyama et al, as described above, because it provides a method to help locate the cause of a problem that occurs during communication [column 1, lines 24-27].

As to claim 14, the Jardin-Fujiyama combination teaches that the entry further includes an initialization vector [Fujiyama et al column 6, lines 56-65].

**10. Claims 13 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 and Fujiyama et al U.S. Patent No. 6,052,728 as applied to claim 12 above, and further in view of Bellaton et al U.S. Patent No. 6,473,425 B1.**

As to claims 13 and 15, the Jardin-Fujiyama combination teaches that the database includes an entry for a session comprising a session ID [Fujiyama et al column 7, lines 58-62].

The Jardin-Fujiyama combination does not teach that the database includes a TCP Sequence number and an SSL session number. The Jardin-Fujiyama combination does not teach that the entry includes an expected ACK.

Bellaton et al teaches entries that include a TCP Sequence number, SSL session number and an expected ACK [column 8 line 53 to column 9 line 20].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Fujiyama combination so that a TCP Sequence number, SSL session number and an expected ACK would have been included in the database entry.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Fujiyama combination by the teaching of Bellaton et al, as described above, because implementing this method and by comparing a new packet to packets already queued for transmission, unnecessary duplicated transmission of a packet can be avoided where packet transmission has been delayed. Avoiding retransmission of the queued packet avoids aggravating the network congestion [column 5 line 66 to column 6 line 7].

**11. Claims 16, 17 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 as applied to claim 1 above, and further in view of Gelman et al U.S. Patent No. 6,415,329 B1.**

As to claims 16 and 17, Jardin teaches receiving encrypted data packets, as discussed above for claim 1.

Jardin does not teach that the step of receiving the encrypted data packets includes receiving data packets including encrypted application data spanning multiple packets, and the step of forwarding includes forwarding a portion of the application data contained in an individual encrypted TCP segments to the server without authentication. Jardin does not teach that the step of authenticating the application data on receipt of all packets including the application data.

Gelman et al teaches receiving packets that includes application data spanning multiple packets, and the step of forwarding includes forwarding a portion of the application data contained in an individual TCP segments to the server without authentication [column 9, lines 16-65]. Gelman et al teaches the step of authenticating the application data on receipt of all packets including the application data [column 9, lines 16-65].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin so that the step of receiving the encrypted data packets would have included receiving the data packets that fragmented the application data. The step of forwarding would have included forwarding a portion of the application data contained in the individual fragmented TCP segments to the server without authentication. The application data would have been authenticated on receipt of all the packets including the application data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin by the teaching of Gelman et al, as described above, because fragmenting the packets maintains a low susceptibility to transmission errors and makes it difficult for a third party to intercept the application [column 2, lines 58-63].

As to claim 19, Jardin teaches that the data is buffered for a length sufficient to complete a block cipher used to encrypt the data [column 7, lines 6-19].

**12. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 and Gelman et al U.S. Patent No. 6,415,329 B1 as applied to claim 16 above, and further in view of Holtey et al U.S. Patent No. 5,293,424.**

As to claim 18, the Jardin-Gelman combination is silent on the data not being buffered during decryption.

Holtey et al teaches data not being buffered during decryption [column 4 line 59 to column 5 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Gelman combination so that the data would not have been buffered during decryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Gelman combination by the teaching of Holtey et al, as described above, because buffering is a time consuming process and the buffered data is subject to attack [column 4 line 59 to column 5 line 2].

**13. Claims 20-22, 27 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellwood et al U.S. Patent No. 6,584,567 B1 in view of Maloney et al U.S. Patent No. 6,253,337 B1.**

As to claim 20, Bellwood et al discloses a method for secure communications between a client and one of a plurality of servers performed on an intermediary device, comprising:

(a) establishing a communications session between the client and the one of the plurality of servers by receiving negotiation data from the client intended for the server and forwarding the negotiation data in modified form to the server,

and receiving negotiation data from the server intended for the client and forwarding the negotiation data to the client [column 4, lines 1-24];

(b) establishing a secure communications session between the client and the intermediary device [column 4, lines 51-64];

(d) receiving encrypted application data from the intermediary device [column 6, lines 10-30];

(e) decrypting the application data [column 6, lines 10-30]; and

(f) forwarding decrypted application data to the one of the plurality of servers [column 6, lines 10-30].

Bellwood et al does not teach:

(c) maintaining a database of the secure communications session including information on the session/packet associations.

Maloney et al teaches maintaining a database of the secure communications session including information on the session/packet associations [column 6, lines 33-51].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Bellwood et al so that the proxy server would have had a log that maintained records of the secure communications session including information on the session/packet associations.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Bellwood et al by the teaching of Maloney et al because without introducing additional traffic on a network, the system produces a virtual picture of network usage and network vulnerabilities. By organizing the inputs of multiple collection

tools into visual schematics, Security Administrators become proactive in assessing network weaknesses and in identifying optimum locations for implementing security measures. With the information revealed by the system of the present invention, Security Administrators can identify potential traffic bottlenecks, locate the existence of backdoors, reduce bandwidth usage, develop profiles of users, and pinpoint illicit activity [column 1, lines 57-67].

As to claim 21, Bellwood et al teaches the method further including the steps of:

- (g) receiving application data from the server [column 5 line 66 to column 6 line 9];
- (h) encrypting the application data [column 5 line 66 to column 6 line 9]; and
- (i) forwarding the application data to the client [column 5 line 66 to column 6 line 9].

As to claim 22, Bellwood et al teaches that the method further includes the step of selecting one of the plurality of servers for each packet in the communications session and mapping all communications intended for the server to the one of the plurality of servers [column 4, lines 51-64].

As to claim 27, the Bellwood-Malone combination teaches that the entry further includes an initialization vector [column 4, lines 1-35].

As to claim 29, Bellwood et al teaches that the step of forwarding includes:

- forwarding data which spans over multiple TCP segments and forwarding data which is not authenticated [column 4, lines 51-64].

**14. Claims 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellwood et al U.S. Patent No. 6,584,567 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 20 above, and further in view of Cohen et al U.S. Patent No. 6,389,462 B1.**

As to claim 23, the Bellwood-Maloney combination does not teach that the step of managing comprises receiving packets from the one of the plurality of servers and modifying the source and destination addresses of the packet to return the packet to the client.

Cohen et al teaches receiving packets from one of the plurality servers and modifying the source and destination addresses of the packet to return the packet to the client [column 9 line 19 to column 10 line 31].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Bellwood-Maloney combination so that the proxy would have received packets from one of the servers and modified the source and destination addresses of the packet to return the packet to the client.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Bellwood-Maloney combination by the teaching of Cohen et al, as described above, because address translation by a proxy server reduces latency and minimizes traffic onto and off of the network [column 1, lines 44-58].

As to claim 24, the Bellwood-Maloney combination teaches that the step of decrypting application comprises decrypting data and forwarding the data on to the one of the plurality of servers via a secure network [Bellwood et al column 6, lines 10-30].

As to claim 25, the Bellwood-Malone combination teaches that the step of receiving application data from the one of the plurality of servers, encrypting the data, and forwarding encrypted data to the client [Bellwood et al column 6, lines 10-30].

**15. Claims 26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellwood et al U.S. Patent No. 6,584,567 B1 and Malone et al U.S. Patent No. 6,253,337 B1 as applied to claim 20 above, and further in view of Bellaton et al U.S. Patent No. 6,473,425 B1.**

As to claims 26 and 28, the Bellwood-Malone combination teaches an entry for a session ID [Malone column 5 line 63 to column 6 line 32].

The Bellwood-Malone combination does not teach that the database includes an entry for a session comprising a TCP Sequence number and an SSL session number. The Bellwood-Malone combination does not teach that the entry includes an expected ACK.

Bellaton et al teaches entries that include a TCP Sequence number, SSL session number and an expected ACK [column 8 line 53 to column 9 line 20].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Bellwood-Malone combination so that a TCP Sequence number, SSL session number and an expected ACK would have been included in the database entry.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Bellwood-Malone combination by the teaching of Bellaton et al, as described above, because implementing this method and by comparing a new packet to packets already queued for transmission, unnecessary duplicated transmission of a

packet can be avoided where packet transmission has been delayed. Avoiding retransmission of the queued packet avoids aggravating the network congestion [column 5 line 66 to column 6 line 7].

**16. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bellwood et al U.S. Patent No. 6,584,567 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 20 above, and further in view of Holtey et al U.S. Patent No. 5,293,424.**

As to claim 30, the Bellwood-Maloney combination does not teach that the data is not buffered during decryption.

Holtey et al teaches data not being buffered during decryption [column 4 line 59 to column 5 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Bellwood-Maloney combination so that the data would not have been buffered during decryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Bellwood-Maloney combination by the teaching of Holtey et al, as described above, because buffering is a time consuming process and the buffered data is subject to attack [column 4 line 59 to column 5 line 2].

**17. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bellwood et al U.S. Patent No. 6,584,567 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 20 above, and further in view of Boeuf U.S. Patent No. 6,009,502.**

As to claim 31, the Bellwood-Maloney combination does not teach that the data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

Boeuf teaches that data is buffered for a length sufficient to complete a block cipher [column 5, lines 21-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Bellwood-Maloney combination so that the data would have been buffered for a length sufficient to complete a block cipher used to encrypt the data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Bellwood-Maloney combination by the teaching of Boeuf, as described above, because it prevents the client from sending data when the server is no longer able to perform normal data storage operations. Such a protocol will operate to limit the amount of client vital data which might be lost [column 2, lines 36-42].

**18. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bellwood et al U.S. Patent No. 6,584,567 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 20 above, and further in view of Weinstein et al U.S. Patent No. 6,094,485.**

As to claim 32, the Bellwood-Maloney combination does not teach that the step of forwarding includes authenticating the decrypted data after a final segment of a multi-segment encrypted data stream is received.

Weinstein et al teaches verifying the decrypted data after a final segment of a multi-segment encrypted data stream is received [column 8, lines 37-64].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Bellwood-Maloney combination so that the

step of forwarding would have included verifying the decrypted data after a final segment of a multi-segment data stream was received.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Bellwood-Malone combination by the teaching of Weinstein et al, as described above, because it validates that none of the segments of data were altered during transmission by a third party.

**19. Claims 33-35, 38, 39 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 in view of Malone et al U.S. Patent No. 6,253,337 B1.**

As to claims 33, 39 and 41, Jardin discloses an apparatus coupled to a public network and a secure network, communicating with a client via the public network and communicating with one of a plurality of servers via the secure network, comprising:

- a network communications interface [column 3, lines 46-60];
- at least one processor [column 3, lines 46-60];
- programmable dynamic memory [column 3, lines 46-60];
- a communications channel coupling the processor, memory and network communications interface [column 3, lines 46-60];
- a client/server open communications session manager [column 4, lines 11-24];
- a client secure communication session manager [column 4, lines 25-34];
- and
- a data packet encryption and decryption engine [column 5, lines 16-30].

Jardin does not teach a client/server secure communications session tracking database.

Maloney et al teaches a client/server secure communications session tracking database [column 6, lines 33-51].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin so that the proxy would have had a client/server secure communications session tracking database.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin by the teaching of Maloney et al because without introducing additional traffic on a network, the system produces a virtual picture of network usage and network vulnerabilities. By organizing the inputs of multiple collection tools into visual schematics, Security Administrators become proactive in assessing network weaknesses and in identifying optimum locations for implementing security measures. With the information revealed by the system of the present invention, Security Administrators can identify potential traffic bottlenecks, locate the existence of backdoors, reduce bandwidth usage, develop profiles of users, and pinpoint illicit activity [column 1, lines 57-67].

As to claim 34, Jardin teaches that the client open communications session manager and secure communication manager enables the apparatus as a TCP and SSL proxy for the server [column 4, lines 34-47].

As to claim 35, Jardin teaches that the communications session managers enable transparent secure and open communication between the client and the server [column 6, lines 4-37].

As to claim 38, Jardin teaches that data packet encryption and decryption engine performs SSL encryption and decryption on data packets transmitted between the client and the at least one server [column 5, lines 16-30].

**20. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Cohen et al U.S. Patent No. 6,389,462 B1.**

As to claim 36, the Jardin-Maloney combination does not teach that the client negotiation managers route packets between the client and the one of the plurality of servers by modifying source and destination addresses.

Cohen et al teaches receiving packets from one of the plurality servers and modifying the source and destination addresses of the packet to return the packet to the client [column 9 line 19 to column 10 line 31].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Maloney combination so that the proxy would have routed packets between the client and one of the servers by modifying the source and destination addresses of the packet.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Maloney combination by the teaching of Cohen et al, as described above, because address translation by a proxy server reduces latency and minimizes traffic onto and off of the network [column 1, lines 44-58].

**21. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Harper et al U.S. Patent No. 6,820,215 B2.**

As to claim 37, the Jardin-Maloney combination does not teach a load selection manager balancing the routing of multiple open and secure communications sessions between a plurality of clients and a plurality of servers.

Harper et al teaches load selection manager balancing the routing of multiple open and secure communications sessions between a plurality of clients and a plurality of servers [column 6, lines 16-29].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Maloney combination so that there would have been a load selection manager balancing the routing of multiple open and secure communications sessions between a plurality of clients and a plurality of servers.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Maloney combination by the teaching of Harper et al, as described above, because it allows heavily accessed Web sites to increase capacity, since multiple server machines can be dynamically added while retaining the abstraction of a single entity that appears in the network as a single logical server. In addition, failure of one or more of the server machines in a server cluster need not completely disable the operation of remainder of the server cluster [column 2, lines 18-33].

**22. Claim 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Bellaton et al U.S. Patent No. 6,473,425 B1.**

As to claim 40, the Jardin-Maloney combination does not teach that the database includes a TCP Sequence number and an SSL session number.

Bellaton et al teaches entries that includes a TCP Sequence number and SSL session number [column 8 line 53 to column 9 line 20].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Maloney combination so that a TCP Sequence number and SSL session number would have been included in the database entry.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Maloney combination by the teaching of Bellaton et al, as described above, because implementing this method and by comparing a new packet to packets already queued for transmission, unnecessary duplicated transmission of a packet can be avoided where packet transmission has been delayed. Avoiding retransmission of the queued packet avoids aggravating the network congestion [column 5 line 66 to column 6 line 7].

**23. Claim 42 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Holtey et al U.S. Patent No. 5,293,424.**

As to claim 42, the Jardin-Maloney combination is silent on the data not being buffered during decryption.

Holtey et al teaches data not being buffered during decryption [column 4 line 59 to column 5 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Malone combination so that the data would not have been buffered during decryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Malone combination by the teaching of Holtey et al, as described above, because buffering is a time consuming process and the buffered data is subject to attack [column 4 line 59 to column 5 line 2].

**24. Claim 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 and Malone et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Boeuf U.S. Patent No. 6,009,502.**

As to claim 43, the Jardin-Malone combination does not teach that the data is buffered for a length sufficient to complete a block cipher used to encrypt the data.

Boeuf teaches that data is buffered for a length sufficient to complete a block cipher [column 5, lines 21-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Malone combination so that the data would have been buffered for a length sufficient to complete a block cipher used to encrypt the data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Malone combination by the teaching of Boeuf,

as described above, because it prevents the client from sending data when the server is no longer able to perform normal data storage operations. Such a protocol will operate to limit the amount of client vital data which might be lost [column 2, lines 36-42].

**25. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 and Maloney et al U.S. Patent No. 6,253,337 B1 as applied to claim 33 above, and further in view of Weinstein et al U.S. Patent No. 6,094,485.**

As to claim 44, the Jardin-Maloney combination does not teach that the step of forwarding includes authenticating the decrypted data after a final segment of a multi-segment encrypted data stream is received.

Weinstein et al teaches verifying the decrypted data after a final segment of a multi-segment encrypted data stream is received [column 8, lines 37-64].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Maloney combination so that the step of forwarding would have included verifying the decrypted data after a final segment of a multi-segment data stream was received.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Jardin-Maloney combination by the teaching of Weinstein et al, as described above, because it validates that none of the segments of data were altered during transmission by a third party.

**26. Claim 49 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 as applied to claim 45 above, and further in view of Holtey et al U.S. Patent No. 5,293,424.**

As to claim 49, Jardin is silent on the data not being buffered during decryption.

Holtey et al teaches data not being buffered during decryption [column 4 line 59 to column 5 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin so that the data would not have been buffered during decryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin by the teaching of Holtey et al, as described above, because buffering is a time consuming process and the buffered data is subject to attack [column 4 line 59 to column 5 line 2].

**27. Claim 50 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin U.S. Patent No. 6,681,327 B1 as applied to claim 45 above, and further in view of Harper et al U.S. Patent No. 6,820,215 B2.**

As to claim 50, Jardin does not teach a load balancing engine.

Harper et al teaches load balancing of servers [column 6, lines 16-29].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin so that the servers would have been load balanced.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Jardin by the teaching of Harper et al, as described above, because it allows heavily accessed Web sites to increase capacity, since multiple server machines can be dynamically added while retaining the abstraction of a single entity that appears in the network as a single logical server. In addition, failure of one or more of the server machines in a server cluster need not completely disable the operation of remainder of the server cluster [column 2, lines 18-33].

*Conclusion*

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy *AM*  
March 10, 2005

*Ayaz Sheikh*  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100